The structure of dual Grassmann codes

Beelen, Peter ; Pinero, Fernando

Published in:
Designs, Codes and Cryptography

Link to article, DOI:
10.1007/s10623-015-0085-3

Publication date:
2016

Document Version
Peer reviewed version

The structure of dual Grassmann codes *

Peter Beelen and Fernando Pinero

Abstract

In this article we study the duals of Grassmann codes, certain codes coming from the Grassmannian variety. Exploiting their structure, we are able to count and classify all their minimum weight codewords. In this classification the lines lying on the Grassmannian variety play a central role. Related codes, namely the affine Grassmann codes, were introduced more recently in [1], while their duals were introduced and studied in [2]. In this paper we also classify and count the minimum weight codewords of the dual affine Grassmann codes. Combining the above classification results, we are able to show that the dual of a Grassmann code is generated by its minimum weight codewords. We use these properties to establish that the increase of value of successive generalized Hamming weights of a dual Grassmann code is 1 or 2.

AMS classification 14G50, 94B27, 14M15

1 Introduction and preliminaries.

The Grassmannian variety is a fundamental mathematical object. It encompasses aspects from algebra, geometry and combinatorics. For example, the Grassmannian variety plays a role in the theory of distance-transitive graphs, finite geometries, network design and coding theory. In this article we are interested in the last of these topics, namely their application in coding theory for the construction of Grassmann codes [8, 10, 11]. Since their introduction, these codes have been a recurring object of study and articles have appeared concerning their minimum distance [8, 12], some of their generalized Hamming weights [3, 4, 6, 8], and their automorphism group [5].

A variation of these codes, the affine Grassmann codes was introduced in [1] and a broader class of codes, the affine Grassmann codes of a specified level, in [2]. In the latter article the duals of affine Grassmann codes were investigated. For future reference we will give a synopsis of the definition of these codes and their properties below. After this we will classify the minimum weight codewords in the dual of both affine Grassmann codes with a specified level and Grassmann codes and give a link with the geometry of the Grassmannian variety. Finally we will use this classification for the following purposes: First of all, to determine the exact number of such minimum weight codewords, secondly to establish that the dual Grassmann code is generated by its minimum weight codewords, thirdly to establish a growth property of the generalized Hamming weights, and finally to describe Grassmann codes in a more combinatorial graph-theoretical way, namely as a Tanner code.

*The authors gratefully acknowledge the support from the Danish National Research Foundation and the National Science Foundation of China (Grant No.11061130539) for the Danish-Chinese Center for Applications of Algebraic Geometry in Coding Theory and Cryptography as well as the support from The Danish Council for Independent Research (Grant No. DFF–4002-00367).

In the remainder of this section we give an overview of the theory of (affine) Grassmann codes and fix the notation that will be used in the remainder of the article. All the material in this overview is contained in [1, 2] and the reader is kindly referred to these articles for further details. All material in the subsequent sections is new unless specified otherwise.

Definition 1 *Let $\boldsymbol{M} = (m_{ij})$ be an $\ell \times \ell'$ matrix, with $\ell \leq \ell'$. Let $I \subseteq \{1, 2, \ldots, \ell\}$ and $J \subseteq \{1, 2, \ldots, \ell'\}$ be subsets both of cardinality h. Then we define the $h \times h$ submatrix of $\boldsymbol{M}$ specified by I and J by*

$$\boldsymbol{M}_{I,J} := (m_{ij})_{i \in I, j \in J}.$$

Further we call $\det \boldsymbol{M}_{I,J}$ *an h-minor of $\boldsymbol{M}$. For the sake of completeness, we define the* 0*-minor of $\boldsymbol{M}$ as* 1*.*

We will write $\mathbb{M}_{\ell \times \ell'}(\mathbb{F}_q)$ for the set of $\ell \times \ell'$ matrices with entries from $\mathbb{F}_q$. Later on, we will evaluate matrices in certain functions. To be closer to the usual language when defining evaluation codes, we will therefore freely identify $\mathbb{M}_{\ell \times \ell'}(\mathbb{F}_q)$ with the set of points of the affine space $\mathbb{A}^\delta(\mathbb{F}_q)$ of dimension $\delta := \ell\ell'$. The coordinate ring of this affine space is a polynomial ring in δ indeterminates X_{ij}, but for convenience, we simply write $\mathbb{F}_q[\mathbf{X}]$, with $\mathbf{X}$, the ℓ times ℓ' matrix whose entries are the indeterminates X_{ij}. Finally, we fix an ordering $P_1, P_2, \ldots, P_{q^\delta}$ of the points of $\mathbb{A}^\delta(\mathbb{F}_q)$ (or equivalently, an ordering of the matrices in $\mathbb{M}^{\ell \times \ell'}(\mathbb{F}_q)$). With these notations and conventions in place, we can start to define affine Grassmann codes, but we first define certain functions and an evaluation map in the following definitions:

Definition 2 *Let $0 \leq h \leq \ell$. We denote the set of h-minors of the matrix of indeterminates $\boldsymbol{X}$ by Δ_h. Further we write*

$$\Delta_{\leq r} := \bigcup_{h=0}^{r} \Delta_h$$

and denote by $\mathcal{F}_r \subset \mathbb{F}_q[\boldsymbol{X}]$ the $\mathbb{F}_q$-linear subspace generated by the elements of $\Delta_{\leq r}$.

Definition 3 *Writing $\delta := \ell\ell'$, we define* $\mathrm{ev} : \mathbb{F}_q[\boldsymbol{X}] \to \mathbb{F}_q^{q^\delta}$ *by*

$$\mathrm{ev}(f(\boldsymbol{X})) := (f(P_1), f(P_2), \ldots, f(P_{q^\delta})).$$

Now that we have both the functions and an evaluation map, we define the following codes as introduced in [1, 2]:

Definition 4 *Let $r \leq \ell \leq \ell'$ be positive integers and define $m := \ell + \ell'$. Then we define the affine Grassmann code of level r by*

$$\mathcal{C}^{\mathbb{A}}(\ell, m; r) := \{\mathrm{ev}(f) \mid f \in \mathcal{F}_r\}.$$

If $r = \ell$, we simply write $\mathcal{C}^{\mathbb{A}}(\ell, m)$ and call it the affine Grassmann code.

Given q, the length of $\mathcal{C}^{\mathbb{A}}(\ell, m; r)$ is simply given by q^δ. The dimension $k^{\mathbb{A}}(\ell, m; r)$ and minimum distance $d^{\mathbb{A}}(\ell, m; r)$ of $\mathcal{C}^{\mathbb{A}}(\ell, m; r)$ can be expressed as follows:

$$k^{\mathbb{A}}(\ell, m; r) = \sum_{i=0}^{r} \binom{\ell}{r} \binom{\ell'}{r} \tag{1}$$

and

$$d^{\mathbb{A}}(\ell, m; r) = q^{\delta} \prod_{i=1}^{r} \left(1 - \frac{1}{q^i}\right). \tag{2}$$

As observed in [2], affine Grassmann codes have several automorphisms. This will be quite useful later on and therefore we describe some of them explicitly below. We use the notation $\mathrm{GL}_h(\mathbb{F}_q)$ for the group of nonsingular $h \times h$ matrices with entries from $\mathbb{F}_q$.

Definition 5 *Let $\boldsymbol{U} \in \mathbb{M}^{\ell \times \ell'}(\mathbb{F}_q)$, $\boldsymbol{A} \in \mathrm{GL}_{\ell'}(\mathbb{F}_q)$ and $\boldsymbol{B} \in \mathrm{GL}_{\ell}(\mathbb{F}_q)$. Then we define the automorphism $\sigma_{\boldsymbol{U},\boldsymbol{A},\boldsymbol{B}} : \mathcal{C}^{\mathbb{A}}(\ell, m; r) \to \mathcal{C}^{\mathbb{A}}(\ell, m; r)$ by*

$$\sigma_{\boldsymbol{U},\boldsymbol{A},\boldsymbol{B}}(\,(f(P_i))_i\,) := (f(\boldsymbol{B}P_i\boldsymbol{A} + \boldsymbol{U}))_i \ \text{ for } \ f \in \mathcal{F}_r.$$

We denote by $\mathfrak{H}(\ell, m)$ the group consisting of such automorphisms.

Note that an element in $\mathfrak{H}(\ell, m)$ acts on a codeword simply by permuting the coordinates of the codeword. As a final preliminary, we paraphrase the results in [2] concerning the dual affine Grassmann codes with a specified level.

Theorem 6 *Let $r \geq 1$ and $\ell \leq \ell'$. The minimum distance $d_{\perp}^{\mathbb{A}}(\ell, m; r)$ of the code $\mathcal{C}^{\mathbb{A}}(\ell, m; r)^{\perp}$ satisfies:*

$$d_{\perp}^{\mathbb{A}}(\ell, m; r) = \begin{cases} 3 & \text{if } q > 2, \\ 4 & \text{if } q = 2 \text{ and } \ell' > 1. \end{cases}$$

Furthermore, $\mathcal{C}^{\mathbb{A}}(\ell, m)^{\perp}$ is generated by its minimum weight codewords.

Note that the minimum distance in the cases that $r = 0$ is trivial to determine, and the resulting codes are of little theoretical interest. If $r = 1$, the codes $\mathcal{C}^{\mathbb{A}}(\ell, m; r)$ and $\mathcal{C}^{\mathbb{A}}(\ell, m; r)^{\perp}$ both fall within the class of generalized Reed–Muller codes, which have been studied extensively. To avoid having to deal with these cases separately all the time, we assume in the remainder of the article that $r \geq 2$. Since $r \leq \ell \leq \ell'$, this implies that all these three integers are always assumed to be at least 2.

If $2 \leq r < \ell$, it is in general not true that $\mathcal{C}^{\mathbb{A}}(\ell, m; r)^{\perp}$ is generated by its minimum weight codewords. In [2] this was shown by giving a counter example with $q = r = 2$ and $\ell = \ell' = 3$. More precisely it was observed in [2] that for $q = 2$ the sets of minimum weight codewords in $\mathcal{C}^{\mathbb{A}}(3, 6; 2)^{\perp}$ and in $\mathcal{C}^{\mathbb{A}}(3, 6)^{\perp}$ are the same, while their dimensions are seen to be distinct using Equation (1) and the usual relation between the dimensions of a code and its dual. As a byproduct of the results in the following section, this observation will be explained fully at the end of the following section. It turns out that a similar phenomenon occurs in general for any value of q and $2 \leq r < \ell \leq \ell'$.

2 Classification of minimum weight codewords of $\mathcal{C}^{\mathbb{A}}(\ell, m; r)^{\perp}$.

As a first new contribution, we classify in this section all minimum weight codewords in the codes $\mathcal{C}^{\mathbb{A}}(\ell, m; r)^{\perp}$ with $2 \leq r \leq \ell \leq \ell'$. While it is already known in case $r = \ell$, that these codewords generate $\mathcal{C}^{\mathbb{A}}(\ell, m; r)^{\perp}$, more information for $r < \ell$ will be obtainable having such a classification. It will be convenient to describe the support of minimum weight codewords. Such a support is in principle just a subset of $\{1, \ldots, q^{\delta}\}$ (indicating in which coordinate positions the non-zero elements occur). However, it will be more convenient to use the points $P_1, \ldots, P_n$ as indices, since the i-th coordinate of a codeword $c = \mathrm{ev}(f)$ simply is given by $f(P_i)$. The points

$P_1, \ldots, P_n$ themselves will as before be identified with $\ell \times \ell'$ matrices from $\mathbb{M}^{\ell \times \ell'}(\mathbb{F}_q)$. All in all, the support of a codeword in $\mathcal{C}^{\mathbb{A}}(\ell, m; r)^{\perp}$ will be described as a set of matrices. It will also turn out to be convenient to have a special notation for some of these matrices:

Definition 7 *Let $2 \leq r \leq \ell \leq \ell'$ and let i and j be integers satisfying $1 \leq i \leq \ell$ and $1 \leq j \leq \ell'$. Then we define $\boldsymbol{E}_{i,j}$ to be the $\ell \times \ell'$ matrix all of whose entries equal 0 except the (i,j)-th entry, which equals 1. Further for $1 \leq \rho \leq \ell$, we write*

$$\boldsymbol{D}_{\rho} := \boldsymbol{E}_{1,1} + \boldsymbol{E}_{2,2} + \cdots \boldsymbol{E}_{\rho,\rho}.$$

We see that

$$\mathbf{D}_{\rho} = \begin{pmatrix} \mathbf{I}_{\rho} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix},$$

where $\mathbf{I}_{\rho}$ denotes the identity matrix of rank ρ. Note that the support of a minimum weight codeword determines the minimum weight codeword itself up to multiplication with a nonzero constant. Indeed if two linearly independent codewords would exist both of minimum weight and with the same support, then a suitable linear combination of the two codewords would give rise to a nonzero codeword of even lower weight, which would be a contradiction.

Already from Theorem 6 one can see that the case $q = 2$ is different from the case $q > 2$. Therefore we will treat these cases separately in two subsections. In both cases however, the group $\mathfrak{H}(\ell, m)$ acts on the set of supports of minimum weight codewords of $\mathcal{C}^{\mathbb{A}}(\ell, m; r)^{\perp}$, giving rise to orbits of supports of minimum weight codewords. The strategy will be to determine these orbits and to single out a representative for each orbit, resulting in a complete description of all possible minimum weight codewords in $\mathcal{C}^{\mathbb{A}}(\ell, m; r)^{\perp}$.

2.1 Classification in case $q \neq 2$.

If $q \neq 2$, the minimum distance of $\mathcal{C}^{\mathbb{A}}(\ell, m; r)^{\perp}$ equals 3 by Theorem 6. A codeword c of minimum weight can therefore be described by its support $\{\mathbf{N}_1, \mathbf{N}_2, \mathbf{N}_3\}$ and the (nonzero) values of the coordinates $c_{\mathbf{N}_1}$, $c_{\mathbf{N}_2}$ and $c_{\mathbf{N}_3}$ of c. Since we have $c \in \mathcal{C}^{\mathbb{A}}(\ell, m; r)^{\perp}$, it holds for any $f \in \mathcal{F}_r$ that

$$c_{\mathbf{N}_1} f(\mathbf{N}_1) + c_{\mathbf{N}_2} f(\mathbf{N}_2) + c_{\mathbf{N}_3} f(\mathbf{N}_3) = 0. \tag{3}$$

Note that by choosing $f = 1$, we immediately obtain that $c_{\mathbf{N}_3} = -(c_{\mathbf{N}_1} + c_{\mathbf{N}_2})$. Using this equation for other choices of f as well, we first show the following theorem:

Theorem 8 *Let $2 \leq r \leq \ell \leq \ell'$ and let $c \in \mathcal{C}^{\mathbb{A}}(\ell, m; r)^{\perp}$ be a weight 3 codeword with support*

$$\mathrm{supp}(c) = \{\boldsymbol{N}_1, \boldsymbol{N}_2, \boldsymbol{N}_3\}.$$

Then there exists $\sigma \in \mathfrak{H}(\ell, m)$ and $\alpha \in \mathbb{F}_q$ such that $c' := \sigma(c)$ has support

$$\mathrm{supp}(c') = \{\boldsymbol{0}, \boldsymbol{D}_1, \alpha \boldsymbol{D}_1\}, \quad \textit{with} \quad \alpha = \frac{c_{\boldsymbol{N}_2}}{c_{\boldsymbol{N}_1} + c_{\boldsymbol{N}_2}}$$

and

$$c'_{\boldsymbol{0}} = c_{\boldsymbol{N}_1}, \; c'_{\boldsymbol{D}_1} = c_{\boldsymbol{N}_2} \textit{ and } c'_{\alpha \boldsymbol{D}_1} = -(c_{\boldsymbol{N}_1} + c_{\boldsymbol{N}_2}).$$

Conversely, given $\alpha \in \mathbb{F}_q \backslash \{0, 1\}$, there exists a codeword $c \in \mathcal{C}^{\mathbb{A}}(\ell, m; r)^{\perp}$ with support $\mathrm{supp}(c) = \{\boldsymbol{0}, \boldsymbol{D}_1, \alpha \boldsymbol{D}_1\}$. Its nonzero coordinates satisfy

$$c_{\boldsymbol{D}_1} = \frac{-\alpha}{\alpha - 1} c_{\boldsymbol{0}} \textit{ and } c_{\alpha \boldsymbol{D}_1} = \frac{1}{\alpha - 1} c_{\boldsymbol{0}}.$$

Proof. Suppose that c satisfies the hypothesis of the theorem. First we consider the codeword $d := \sigma_{\mathbf{N}_1,\mathbf{I}_{\ell'},\mathbf{I}_\ell}(c)$. Then

$$\mathrm{supp}(d) = \{\mathbf{0}, \mathbf{N}_2 - \mathbf{N}_1, \mathbf{N}_3 - \mathbf{N}_1\}$$

and

$$d_{\mathbf{0}} = c_{\mathbf{N}_1},\ d_{\mathbf{N}_2-\mathbf{N}_1} = c_{\mathbf{N}_2} \text{ and } d_{\mathbf{N}_3-\mathbf{N}_1} = c_{\mathbf{N}_3} = -(c_{\mathbf{N}_1} + c_{\mathbf{N}_2}).$$

To simplify the notation we let $\mathbf{M} = \mathbf{N}_2 - \mathbf{N}_1$ and $\mathbf{N} = \mathbf{N}_3 - \mathbf{N}_1$.

For integers i and j such that $1 \leq i \leq \ell$ and $1 \leq j \leq \ell'$, let $f = \det(\mathbf{X}_{\{i\},\{i\}})$. For this choice of f equation (3) implies that $d_{\mathbf{M}}\mathbf{M}_{i,j} + d_{\mathbf{N}}\mathbf{N}_{i,j} = 0$ or in other words that $\mathbf{N}_{i,j} = c_{\mathbf{N}_2}/(c_{\mathbf{N}_1} + c_{\mathbf{N}_2})\mathbf{M}_{i,j}$. Since this equation holds for all possible i and j, we obtain that

$$\mathbf{N} = \frac{c_{\mathbf{N}_2}}{c_{\mathbf{N}_1} + c_{\mathbf{N}_2}}\mathbf{M}. \tag{4}$$

Now let $f = det(\mathbf{X}_{I,J})$ be any 2-minor, then equation (3) applied to the codeword d implies that

$$0 = c_{\mathbf{N}_2} f(\mathbf{M}) - (c_{\mathbf{N}_1} + c_{\mathbf{N}_2}) f(\mathbf{N}) = c_{\mathbf{N}_2} f(\mathbf{M}) - (c_{\mathbf{N}_1} + c_{\mathbf{N}_2}) \left(\frac{c_{\mathbf{N}_2}}{c_{\mathbf{N}_1} + c_{\mathbf{N}_2}}\right)^2 f(\mathbf{M}).$$

In the last equality we used equation (4) and the fact that f is a 2-minor. Simplifying and using that $c_{\mathbf{N}_1} \neq 0$, $c_{\mathbf{N}_2} \neq 0$ and $-(c_{\mathbf{N}_1} + c_{\mathbf{N}_2}) = c_{\mathbf{N}_3} \neq 0$, we obtain that $f(\mathbf{M}) = 0$. Since this holds for any 2-minor, we conclude that $\mathbf{M}$ has rank 1. Since $\mathrm{rank}\mathbf{M} = 1$, there exist matrices $\mathbf{B} \in \mathrm{GL}_\ell(\mathbb{F}_q)$ and $\mathbf{A} \in \mathrm{GL}_{\ell'}(\mathbb{F}_q)$ such that $\mathbf{B}\mathbf{D}_1\mathbf{A} = \mathbf{M}$. Then the codeword $c' := \sigma_{\mathbf{0},\mathbf{A},\mathbf{B}}(d)$ has the desired properties.

What is left is to show the final converse statement. However, a direct verification shows that the codeword of weight three with nonzero entries satisfying the relations stated in the theorem is an element of $\mathcal{C}^{\mathbb{A}}(\ell, m; r)^\perp$. Note that one only needs to check equation (3) for the 0-minor and the 1-minor X_{11}, since all other minors $f \in \mathcal{F}_r$ are zero for the three matrices in the set $\{\mathbf{0}, \mathbf{D}_1, \alpha\mathbf{D}_1\}$. ■

With this classification in place, it will be a fairly easy matter to determine the number of weight three codewords in $\mathcal{C}^{\mathbb{A}}(\ell, m; r)^\perp$. The key ingredient will be the geometric observation obtained from Theorem 8 that the support of a minimum weight codeword lies on a line (i.e. the coset of a one-dimensional subspace of $\mathbb{M}^{\ell\times\ell'}(\mathbb{F}_q)$).

Corollary 2.1 *Let $2 \leq r \leq \ell \leq \ell'$. There are*

$$\frac{q^\delta(q-2)(q^\ell-1)(q^{\ell'}-1)}{6}$$

codewords of weight 3 in $\mathcal{C}^{\mathbb{A}}(\ell, m; r)^\perp$.

Proof. Let $c \in \mathcal{C}^{\mathbb{A}}(\ell, m; r)^\perp$ be a minimum weight codeword. Theorem 8 implies that there exist matrices $\mathbf{U} \in \mathbb{M}^{\ell\times\ell'}(\mathbb{F}_q)$, $\mathbf{A} \in \mathrm{GL}_{\ell'}(\mathbb{F}_q)$ and $\mathbf{B} \in \mathrm{GL}_\ell(\mathbb{F}_q)$ and $\alpha \in \mathbb{F}_q\backslash\{0,1\}$ such that $\mathrm{supp}(\sigma_{\mathbf{U},\mathbf{A},\mathbf{B}}(c)) = \{\mathbf{0}, \mathbf{D}_1, \alpha\mathbf{D}_1\}$. This means that

$$\mathrm{supp}(c) = \{\mathbf{U}, \mathbf{U} + \mathbf{B}\mathbf{D}_1\mathbf{A}, \mathbf{U} + \alpha\mathbf{B}\mathbf{D}_1\mathbf{A}\}.$$

Defining $\mathbf{M} := \mathbf{B}\mathbf{D}_1\mathbf{A}$, we obtain $\mathrm{supp}(c) = \{\mathbf{U}, \mathbf{U}+\mathbf{M}, \mathbf{U}+\alpha\mathbf{M}\}$. In the first place note that this set is contained in a coset of the one-dimensional subspace $\{\beta\mathbf{M} \,|\, \beta \in \mathbb{F}_q\}$ of $\mathbb{M}^{\ell\times\ell'}(\mathbb{F}_q)$. In the second place note that $\mathrm{rank}\mathbf{M} = 1$ and that any such matrix can be written in the form $\mathbf{b}^T\mathbf{a}$ with $\mathbf{a} \in \mathbb{F}_q^{\ell'}$ and $\mathbf{b} \in \mathbb{F}_q^{\ell}$. This description is unique up to multiplying $\mathbf{b}$ and simultaneously dividing

a with a nonzero scalar. Therefore, there exist $(q^\ell - 1)(q^{\ell'} - 1)/(q - 1)$ rank one matrices and consequently $(q^\ell - 1)(q^{\ell'} - 1)/(q-1)^2$ distinct one-dimensional subspaces of $\mathbb{M}^{\ell \times \ell'}(\mathbb{F}_q)$ generated by a rank one matrix. Any such subspace has $q^{\delta-1}$ cosets, giving rise to $q^{\delta-1}(q^\ell - 1)(q^{\ell'} - 1)/(q - 1)^2$ distinct cosets in total.

All possible support sets are obtained by choosing three distinct matrices from the cosets described above. Indeed by the second part of Theorem 8 any choice gives rise to a valid support set. Therefore the total number of distinct support sets is

$$\binom{q}{3} \frac{q^{\delta-1}(q^\ell - 1)(q^{\ell'} - 1)}{(q-1)^2}.$$

Finally, the number of minimum weight codewords is simply $q - 1$ times this amount, since the support of a minimum weight codeword determines it up to multiplication with a nonzero scalar. ■

Note that this formula also correctly counts the number of weight 3 codewords of $\mathcal{C}^{\mathbb{A}}(\ell, m; r)^\perp$ over $\mathbb{F}_2$. Since that code has minimum distance 4, there are no weight three codewords and indeed the formula in Corollary 2.1 evaluates to 0 for $q = 2$.

2.2 Classification in case $q = 2$.

If $q = 2$, the classification of codewords of $\mathcal{C}^{\mathbb{A}}(\ell, m; r)^\perp$ of minimum weight 4 is somewhat more involved than the classification of weight 3 codewords in the previous subsection. This is essentially because the geometric description of the possible support sets turns out to be more complicated. Nevertheless we will see that a similar geometric description can be obtained, but now it involves two lines instead of just one. We will proceed as before by first obtaining explicit and simple representatives of the possible support sets of minimum weight codewords under the action of the group $\mathfrak{H}(\ell, m)$

The support $\mathrm{supp}(c)$ of $c \in \mathcal{C}^{\mathbb{A}}(\ell, m; r)^\perp$ of minimum weight is a set of the form

$$\{\mathbf{M}_1, \mathbf{M}_2, \mathbf{M}_3, \mathbf{M}_4\} \subset \mathbb{M}^{\ell \times \ell'}(\mathbb{F}_2).$$

Since $c \in \mathcal{C}^{\mathbb{A}}(\ell, m; r)^\perp$ and $q = 2$, it holds for any $f \in \mathcal{F}_r$ that

$$f(\mathbf{M}_1) + f(\mathbf{M}_2) + f(\mathbf{M}_3) + f(\mathbf{M}_4) = 0. \tag{5}$$

Note that any nonzero coefficient of a codeword necessarily equals 1, since $q = 2$. As for the case $q = 2$, instead of studying the restrictions imposed on $\mathbf{M}_1$, $\mathbf{M}_2$, $\mathbf{M}_3$, and $\mathbf{M}_4$ by equation (5) directly, we use the action of $\mathfrak{H}(\ell, m)$ to simplify the form of these matrices. Since there are more steps in this simplification when $q \neq 2$, we will divide these steps in several lemmas to improve the clarity of the exposition.

Lemma 9 *Let $c \in \mathcal{C}^{\mathbb{A}}(\ell, m; r)^\perp$ where $\mathrm{supp}(c) = \{\boldsymbol{M}_1, \boldsymbol{M}_2, \boldsymbol{M}_3, \boldsymbol{M}_4\}$ then there exists a codeword $c' \in \mathcal{C}^{\mathbb{A}}(\ell, m; r)^\perp$ such that*

$$\mathrm{supp}(c') = \{\boldsymbol{0}, \boldsymbol{M}_2 + \boldsymbol{M}_1, \boldsymbol{M}_3 + \boldsymbol{M}_1, \boldsymbol{M}_4 + \boldsymbol{M}_1\}.$$

Proof. We use one of the automorphisms defined in Definition 5, namely $\sigma_{\mathbf{M}_1, \mathbf{I}_{\ell'}, \mathbf{I}_\ell}$. Then the codeword $c' := \sigma_{\mathbf{M}_1, \mathbf{I}_{\ell'}, \mathbf{I}_\ell}(c)$ has the desired property. ■

With this lemma in mind, we return to the study of equation (5). We first study this equation in case f is a 1-minor.

Lemma 10 *Let* $c \in \mathcal{C}^{\mathbb{A}}(\ell, m; r)^{\perp}$ *such that* $\mathrm{supp}(c) = \{\boldsymbol{0}, \boldsymbol{M}_1, \boldsymbol{M}_2, \boldsymbol{M}_3\}$ *then*

$$\boldsymbol{M}_1 + \boldsymbol{M}_2 = \boldsymbol{M}_3.$$

Proof. Let $f = \det(\mathbf{X}_{\{i\},\{j\}}) = X_{ij}$ for arbitrary i and j satisfying $1 \leq i \leq \ell$ and $1 \leq j \leq \ell'$. Since $r \geq 1$ (since throughout we assume $r \geq 2$), we see from equation (5) that $(\mathbf{M}_1)_{i,j} + (\mathbf{M}_2)_{i,j} + (\mathbf{M}_3)_{i,j} = 0$. Since i and j were arbitrary and $q = 2$, we obtain $\mathbf{M}_1 + \mathbf{M}_2 = \mathbf{M}_3$. ■

Note that this lemma could also have been shown using the theory of (binary) Reed–Muller codes. Indeed it is well known that the supports of minimum weight codewords in a binary Reed–Muller code $\mathrm{RM}(a, \delta)$ are very structured: they can be identified with affine $(\delta - a)$-dimensional linear subspaces (flats) of the affine space $\mathbb{A}^{\delta}(\mathbb{F}_2)$; see for example Thm. 13.4.5 in [7]. Since one can show that $\mathcal{C}^{\mathbb{A}}(\ell, m; r)^{\perp}$ is a subcode of $\mathrm{RM}(\delta - 2, \delta)$ both of which have minimum distance four, any minimum weight codeword of $\mathcal{C}^{\mathbb{A}}(\ell, m; r)^{\perp}$ is a minimum weight codeword of $\mathrm{RM}(\delta - 2, \delta)$. The support of these minimum weight codewords can therefore be identified with a flat of dimension two. This is in essence the combined statements of Lemmas 9 and 10.

We continue our study of minimum weight codewords by finding a codeword of minimum weight with an even simpler support than the described Lemma 10.

Lemma 11 *Let* $c \in \mathcal{C}^{\mathbb{A}}(\ell, m; r)^{\perp}$ *where* $supp(c) = \{\boldsymbol{0}, \boldsymbol{M}_1, \boldsymbol{M}_2, \boldsymbol{M}_1 + \boldsymbol{M}_2\}$ *and define*

$$\rho := \min\{\mathrm{rank}\boldsymbol{M}_1, \mathrm{rank}\boldsymbol{M}_2, \mathrm{rank}(\boldsymbol{M}_1 + \boldsymbol{M}_2)\}.$$

Then there exists a codeword $c' \in \mathcal{C}^{\mathbb{A}}(\ell, m; r)^{\perp}$ *and a matrix* $\boldsymbol{M} \in \mathbb{M}^{\ell \times \ell'}(\mathbb{F}_2)$ *with* $\boldsymbol{M}_{1,1} = 0$, $\mathrm{rank}\boldsymbol{M} \geq \rho$ *and* $\mathrm{rank}(\boldsymbol{D}_\rho + \boldsymbol{M}) \geq \rho$, *such that*

$$supp(c') = \{\boldsymbol{0}, \boldsymbol{D}_\rho, \boldsymbol{M}, \boldsymbol{D}_\rho + \boldsymbol{M}\}.$$

Proof. Note that $\rho > 0$, since all matrices in the support are distinct and hence the zero matrix only occurs once in $\mathrm{supp}(c)$. Moreover, without loss of generality we may assume that $\rho = \mathrm{rank}\mathbf{M}_1$. Then there exist matrices $\mathbf{B} \in \mathrm{GL}_\ell(\mathbb{F}_2)$ and $\mathbf{A} \in \mathrm{GL}_{\ell'}(\mathbb{F}_2)$ such that $\mathbf{B}\mathbf{D}_\rho\mathbf{A} = \mathbf{M}_1$, with $\mathbf{D}_\rho$ as in Definition 7. Then the codeword $c' := \sigma_{\mathbf{0},\mathbf{A},\mathbf{B}}(c)$ has support

$$\mathrm{supp}(c') = \{\mathbf{0}, \mathbf{D}_\rho, \mathbf{B}^{-1}\mathbf{M}_2\mathbf{A}^{-1}, \mathbf{D}_\rho + \mathbf{B}^{-1}\mathbf{M}_2\mathbf{A}^{-1}\}.$$

Note that ranks of the matrices in the supports of c and c' have not changed under the automorphism, since $\mathbf{A}$ and $\mathbf{B}$ are regular matrices. Therefore $\mathbf{D}_\rho$ is the matrix of smallest rank among the non-zero matrices occurring in $\mathrm{supp}(c')$.

Moreover, since $\rho > 0$, the $(1,1)$-th entry of either $\mathbf{B}^{-1}\mathbf{M}_2\mathbf{A}^{-1}$ or the matrix $\mathbf{D}_\rho + \mathbf{B}^{-1}\mathbf{M}_2\mathbf{A}^{-1}$ equals zero. Choosing $\mathbf{M}$ to be the matrix among these two having 0 as $(1,1)$-th entry, the lemma follows. ■

Now we look at the restrictions the 2-minors impose on ρ and $\mathbf{M}$ when considering equation (5).

Lemma 12 *Let* $c \in \mathcal{C}^{\mathbb{A}}(\ell, m; r)^{\perp}$ *such that* $supp(c) = \{\boldsymbol{0}, \boldsymbol{D}_\rho, \boldsymbol{M}, \boldsymbol{D}_\rho + \boldsymbol{M}\}$ *as in Lemma 11. Then* $\boldsymbol{M}_{i,i} = 0$ *for any integer satisfying* $1 \leq i \leq \rho$.

Proof. Note that $\mathbf{M}_{1,1} = 0$ by Lemma 11. Let $f = \det(\mathbf{X}_{\{1,i\},\{1,i\}})$. If $1 < i \leq \rho$ we have

$$f(\mathbf{0}) = 0,\ f(\mathbf{D}_\rho) = 1,\ f(\mathbf{M}) = \mathbf{M}_{1,i}\mathbf{M}_{i,1},\ f(\mathbf{M} + \mathbf{D}_\rho) = \mathbf{M}_{i,i} + 1 + \mathbf{M}_{1,i}\mathbf{M}_{i,1}.$$

Therefore equation (5) implies that $\mathbf{M}_{i,i} = 0$. ■

This takes care of some of the diagonal entries of $\mathbf{M}$. The remaining diagonal entries, as well as most other entries of $\mathbf{M}$, are determined in the next lemma.

Lemma 13 *Let $c \in \mathcal{C}^{\mathbb{A}}(\ell, m; r)^{\perp}$ such that supp$(c) = \{\boldsymbol{0}, \boldsymbol{D}_\rho, \boldsymbol{M}, \boldsymbol{D}_\rho + \boldsymbol{M}\}$. Let $i > 1$ and $j > 1$ be integers and suppose $i > \rho$ or $j > \rho$. Then $\boldsymbol{M}_{i,j} = 0$.*

Proof. We consider the 2-minor $f = \det(\mathbf{X}_{\{1,i\},\{1,j\}})$ where $i > \rho$ or $j > \rho$. In this case

$$f(\mathbf{0}) = 0,\ f(\mathbf{D}_\rho) = 0,\ f(\mathbf{M}) = \mathbf{M}_{1,j}\mathbf{M}_{i,1},\ f(\mathbf{M} + \mathbf{D}_\rho) = \mathbf{M}_{i,j} + \mathbf{M}_{1,j}\mathbf{M}_{i,1}.$$

Equation (5) implies the desired result. ■

We have now proven that if there is a codeword in $\mathcal{C}^{\mathbb{A}}(\ell, m; r)^{\perp}$ with support in $\{\mathbf{0}, \mathbf{D}_\rho, \mathbf{M}, \mathbf{D}_\rho + \mathbf{M}\}$ then the entries of the four matrices are 0 if they are not lying in the first row, the first column or in the $\rho \times \rho$ submatrix determined by the first ρ rows and columns. We now prove that in fact $\rho = 1$, which will imply that undetermined entries in $\mathbf{M}$ are restricted to its first row and column.

Lemma 14 *Let $c \in \mathcal{C}^{\mathbb{A}}(\ell, m; r)^{\perp}$ such that supp$(c) = \{\boldsymbol{0}, \boldsymbol{D}_\rho, \boldsymbol{M}, \boldsymbol{D}_\rho + \boldsymbol{M}\}$, with ρ and $\boldsymbol{M}$ as in Lemma 11. Then $\rho = 1$.*

Proof. First of all, let us assume that $\rho \geq 2$. We'll show that $\mathbf{M}_{i,1} = \mathbf{M}_{1,j} = 0$ for all $i > 2$ and $j > 2$. We consider the 2-minor $f = \det(\mathbf{X}_{\{1,2\},\{2,j\}})$ with $j > 2$. Note that Lemma 12 implies $\mathbf{M}_{2,2} = 0$. In this case

$$f(\mathbf{0}) = 0,\ f(\mathbf{D}_\rho) = 0,\ f(\mathbf{M}) = \mathbf{M}_{1,2}\mathbf{M}_{2,j},\ f(\mathbf{M} + \mathbf{D}_\rho) = \mathbf{M}_{1,j} + \mathbf{M}_{1,2}\mathbf{M}_{2,j}.$$

Equation (5) implies that $\mathbf{M}_{1,j} = 0$ for any $j > 2$. Similarly we may prove $\mathbf{M}_{i,1} = 0$ whenever $i > 2$.

If $\rho = 2$, the above combined with Lemmas 12 and 13 implies that $\mathbf{M}$ may have nonzero entries only in positions $(1, 2)$ and $(2, 1)$. By the remark after Lemma 11, $\rho = 2$ is the minimal rank among the matrices $\mathbf{D}_2$, $\mathbf{M}$ and $\mathbf{D}_2 + \mathbf{M}$. Therefore (using $q = 2$) $\mathbf{M}_{1,2} = \mathbf{M}_{2,1} = 1$. However, this implies that the matrix $\mathbf{D}_2 + \mathbf{M}$ has rank 1, a contradiction. Therefore $\rho = 2$ is not possible.

Now let us assume that $\rho \geq 3$. We will show that this implies that rank$\mathbf{M} \leq 2$, which again will give a contradiction by the remark after Lemma 11. We consider the 2-minor $f = \det(\mathbf{X}_{\{1,i\},\{1,j\}})$ where $1 < i < j \leq \rho$. In this case

$$f(\mathbf{0}) = 0,\ f(\mathbf{D}_\rho) = 0,\ f(\mathbf{M}) = \mathbf{M}_{1,j}\mathbf{M}_{i,1},\ f(\mathbf{M} + \mathbf{D}_\rho) = \mathbf{M}_{i,j} + \mathbf{M}_{1,j}\mathbf{M}_{i,1}.$$

Equation (5) then implies that $\mathbf{M}_{i,j} = 0$. Similarly we may prove $\mathbf{M}_{i,j} = 0$ in case $1 < j < i \leq \rho$. Combining this with the first part of the proof and Lemmas 13 and 12, we see that $\mathbf{M}$ may have nonzero entries only in its $(1, 2)$-th and $(2, 1)$-th position. This implies that $\mathbf{M}$ has rank at most two, a contradiction. ■

We have now gathered enough information to state and prove our classification of (the supports of) weight 4 codewords of $\mathcal{C}^{\mathbb{A}}(\ell, m; r)^{\perp}$. We use notation introduced in Definition 7.

Theorem 15 *Let $2 \leq r \leq \ell \leq \ell'$ and let c be a codeword of $\mathcal{C}^{\mathbb{A}}(\ell, m; r)^{\perp}$ of minimum weight 4. Suppose that*

$$\text{supp}(c) = \{\boldsymbol{M}_1, \boldsymbol{M}_2, \boldsymbol{M}_3, \boldsymbol{M}_4\}.$$

There exists an automorphism $\sigma \in \mathfrak{H}(\ell, m)$ such that supp$(\sigma(c))$ *is one of the following:*

i) $\{\boldsymbol{0}, \boldsymbol{D}_1, \boldsymbol{E}_{1,2}, \boldsymbol{D}_1 + \boldsymbol{E}_{1,2}\}$,

ii) $\{\boldsymbol{0}, \boldsymbol{D}_1, \boldsymbol{E}_{2,1}, \boldsymbol{D}_1 + \boldsymbol{E}_{2,1}\}$,

iii) $\{\boldsymbol{0}, \boldsymbol{D}_1, \boldsymbol{E}_{1,2} + \boldsymbol{E}_{2,1}, \boldsymbol{D}_1 + \boldsymbol{E}_{1,2} + \boldsymbol{E}_{2,1}\}$.

Proof. Given c as in the theorem, we know by Lemmas 11 and 14 that there exists $\tau \in \mathfrak{H}(\ell, m)$ such that $\mathrm{supp}(\tau(c)) = \{\mathbf{0}, \mathbf{D}_1, \mathbf{M}, \mathbf{D}_1 + \mathbf{M}\}$, with $\mathbf{M}$ a matrix such that $\mathbf{M}_{1,1} = 0$. Moreover, by Lemma 13, we know that $\mathbf{M}_{i,j} = 0$ if $i \geq 1$ and $j \geq 1$. This implies that the only nonzero entries of $\mathbf{M}$ may occur in its first row or first column, but not in position $(1,1)$. We can therefore perform elementary row and column operations that simplify the first row and column of $\mathbf{M}$, but leave $\mathbf{D}_1$ intact. More precisely, if the first row (or column) contains a 1, we may simplify this row (or column) by moving the 1 to position $(1,2)$ (or $(2,1)$), while removing all other nonzero entries in the row (or column). In other words, we can find matrices $\mathbf{A} \in \mathrm{GL}_{\ell'}(\mathbb{F}_q)$ and $\mathbf{B} \in \mathrm{GL}_{\ell}(\mathbb{F}_q)$ such that $\mathbf{B}^{-1}\mathbf{D}_1\mathbf{A}^{-1} = \mathbf{D}_1$ and $\mathbf{B}^{-1}\mathbf{M}\mathbf{A}^{-1} \in \{\mathbf{E}_{1,2}, \mathbf{E}_{2,1}, \mathbf{E}_{1,2} + \mathbf{E}_{2,1}\}$. The automorphism $\sigma := \sigma_{\mathbf{0},\mathbf{A},\mathbf{B}} \circ \tau$ then has the desired property. ■

The three cases in the above theorem are representatives of all possible orbits of supports of weight 4 codewords of $\mathcal{C}^{\mathbb{A}}(\ell, m; r)^{\perp}$ arising under the action of the group $\mathfrak{H}(\ell, m)$. This means we can describe any support of a minimum weight codeword rather explicitly. We state this in the following corollary:

Corollary 2.2 *Let $q = 2$ and $2 \leq r \leq \ell \leq \ell'$. Then the support of a minimum weight codeword of $\mathcal{C}^{\mathbb{A}}(\ell, m; r)^{\perp}$ is among one of the following three distinct classes of supports:*

i) $\{\boldsymbol{U}, \boldsymbol{U} + \boldsymbol{b}_1^T\boldsymbol{a}_1, \boldsymbol{U} + \boldsymbol{b}_1^T\boldsymbol{a}_2, \boldsymbol{U} + \boldsymbol{b}_1^T(\boldsymbol{a}_1 + \boldsymbol{a}_2)\}$,

ii) $\{\boldsymbol{U}, \boldsymbol{U} + \boldsymbol{b}_1^T\boldsymbol{a}_1, \boldsymbol{U} + \boldsymbol{b}_2^T\boldsymbol{a}_1, \boldsymbol{U} + (\boldsymbol{b}_1 + \boldsymbol{b}_2)^T\boldsymbol{a}_1\}$,

iii) $\{\boldsymbol{U}, \boldsymbol{U} + \boldsymbol{b}_1^T\boldsymbol{a}_1, \boldsymbol{U} + \boldsymbol{b}_1^T\boldsymbol{a}_2 + \boldsymbol{b}_2^T\boldsymbol{a}_1, \boldsymbol{U} + (\boldsymbol{b}_1^T\boldsymbol{a}_1 + \boldsymbol{b}_2^T\boldsymbol{a}_1 + \boldsymbol{b}_1^T\boldsymbol{a}_2)\}$.

Here $\boldsymbol{U} \in \mathbb{M}^{\ell \times \ell'}(\mathbb{F}_2)$, while $\{\boldsymbol{a}_1, \boldsymbol{a}_2\} \subset \mathbb{F}_2^{\ell'}$ and $\{\boldsymbol{b}_1, \boldsymbol{b}_2\} \subset \mathbb{F}_2^{\ell}$ are two pairs of linearly independent vectors. Conversely, any such set occurs as the support set of a minimum weight codeword in $\mathcal{C}^{\mathbb{A}}(\ell, m; r)^{\perp}$.

Proof. Acting on the three representatives from Theorem 15 with $\sigma_{\mathbf{U},\mathbf{A},\mathbf{B}}$ gives a description of all possible support sets. The matrix $\mathbf{M} := \mathbf{B}\mathbf{D}_1\mathbf{A}$ is of the form $\mathbf{M} = \mathbf{b}_1^T\mathbf{a}_1$ for certain non-zero vectors $\mathbf{b}_1, \mathbf{a}_1$. In fact $\mathbf{b}_1^T$ is the first column of $\mathbf{B}$ and $\mathbf{a}_1$ is first row of $\mathbf{A}$. Similarly $\mathbf{B}\mathbf{E}_{1,2}\mathbf{B} = \mathbf{b}_1^T\mathbf{a}_2$ and $\mathbf{B}\mathbf{E}_{2,1}\mathbf{B} = \mathbf{b}_2^T\mathbf{a}_1$, with $\mathbf{b}_2^T$ (resp. $\mathbf{a}_2$) the second column of $\mathbf{B}$ (resp. the second row of $\mathbf{A}$). Note that $\mathbf{b}_1$ and $\mathbf{b}_2$ (resp. $\mathbf{a}_1$ and $\mathbf{a}_2$) necessarily are linearly independent, since $\mathbf{B}$ (resp. $\mathbf{A}$) is an invertible matrix. This shows the first part of the corollary. Since $\mathbf{A}$ and $\mathbf{B}$ may be chosen freely any set of the given three forms occurs as the support set of a minimum weight codeword. ■

A geometric description of this corollary is that the support sets lie on a coset of certain subspaces of $\mathbb{M}^{\ell \times \ell'}(\mathbb{F}_2)$ of dimension two. The subspaces are not arbitrary, but are generated by matrices of a specific form. This enables us to count the number of weight 4 codewords in $\mathcal{C}^{\mathbb{A}}(\ell, m; r)^{\perp}$.

Corollary 2.3 *Let $q = 2$ and assume that $2 \leq r \leq \ell \leq \ell'$. The number of minimum weight 4 codewords in $\mathcal{C}^{\mathbb{A}}(\ell, m; r)^{\perp}$ equals*

$$\frac{(2^{\ell} - 1)(2^{\ell'} - 1)2^{\delta - 2}}{3}\left((2^{\ell-1} - 1) + (2^{\ell'-1} - 1) + 3(2^{\ell-1} - 1)(2^{\ell'-1} - 1)\right).$$

Proof. We first count the number of possible supports of type i): As a first step we determine the number of possibilities for the 2-dimensional subspace

$$W_1 := \{\mathbf{0}, \mathbf{b}_1^T\mathbf{a}_1, \mathbf{b}_1^T\mathbf{a}_2, \mathbf{b}_1^T(\mathbf{a}_1 + \mathbf{a}_2)\}.$$

We may choose $\mathbf{b}_1$ in $2^\ell - 1$ distinct ways. Rather than choosing the vectors $\mathbf{a}_1$ and $\mathbf{a}_2$, we simply choose a 2-dimensional subspace of $\mathbb{F}_2^{\ell'}$. This can be done in $(2^{\ell'}-1)(2^{\ell'}-2)/6$ ways. For W_1 there are therefore the following number of possible choices:

$$\frac{(2^\ell - 1)(2^{\ell'} - 1)(2^{\ell'-1} - 1)}{3}.$$

Since each W_1 has exactly $2^{\delta-2}$ distinct cosets, this gives a total of

$$\frac{2^{\delta-2}(2^\ell - 1)(2^{\ell'} - 1)(2^{\ell'-1} - 1)}{3}$$

possibilities for the support in case i). Similarly in case ii) one obtains

$$\frac{2^{\delta-2}(2^{\ell'} - 1)(2^\ell - 1)(2^{\ell-1} - 1)}{3}$$

possibilities.

The last case left to investigate is case iii). We first wish to determine the number of possibilities for

$$W_2 := \{\mathbf{0}, \mathbf{b}_1^T\mathbf{a}_1, \mathbf{b}_1^T\mathbf{a}_2 + \mathbf{b}_2^T\mathbf{a}_1, \mathbf{b}_1^T\mathbf{a}_1 + \mathbf{b}_1^T\mathbf{a}_2 + \mathbf{b}_2^T\mathbf{a}_1\}.$$

Note that W_2 contains exactly one matrix of rank one, which is determined uniquely by choosing $\mathbf{b}_1$ and $\mathbf{a}_1$ since $q = 2$. Therefore the rank one matrix can be chosen in $(2^\ell - 1)(2^{\ell'} - 1)$ distinct ways. The vector $\mathbf{b}_2$ (resp. $\mathbf{a}_2$) should be chosen linearly independent from $\mathbf{b}_1$ (resp. $\mathbf{a}_1$) and there are as such $2^{\ell'-2}$ (resp. $2^{\ell'} - 2$) possibilities. However, different choices can give rise to the same subspace W_2. If

$$\mathbf{b}_1^T\mathbf{a}_2 + \mathbf{b}_2^T\mathbf{a}_1 = \mathbf{b}_1^T\mathbf{a}_2' + (\mathbf{b}_2')^T\mathbf{a}_1,$$

then

$$\mathbf{b}_1^T(\mathbf{a}_2 + \mathbf{a}_2') = (\mathbf{b}_2 + \mathbf{b}_2')^T\mathbf{a}_1,$$

implying that $\mathbf{a}_2 + \mathbf{a}_2' = 0$ and $\mathbf{b}_2 + \mathbf{b}_2' = 0$ or that $\mathbf{a}_2 + \mathbf{a}_2' = \mathbf{a}_1$ and $\mathbf{b}_1 = \mathbf{b}_2 + \mathbf{b}_2'$. Similarly if

$$\mathbf{b}_1^T\mathbf{a}_1 + \mathbf{b}_1^T\mathbf{a}_2 + \mathbf{b}_2^T\mathbf{a}_1 = \mathbf{b}_1^T\mathbf{a}_2' + (\mathbf{b}_2')^T\mathbf{a}_1,$$

then either $\mathbf{a}_2' = \mathbf{a}_1 + \mathbf{a}_2 = 0$ and $\mathbf{b}_2' = \mathbf{b}_2 = 0$ or $\mathbf{a}_2' = \mathbf{a}_2$ and $\mathbf{b}_2' = \mathbf{b}_1 + \mathbf{b}_2$. This brings the total number of possibilities for the choice of W_2 to:

$$\frac{(2^\ell - 1)(2^{\ell'} - 1)(2^\ell - 2)(2^{\ell'} - 2)}{4}.$$

The rest of the counting is then done as before. Adding all contributions from the three cases together, one obtains the corollary. ■

Note that for both the case $q = 2$ and $q \neq 2$ the number of minimum weight codewords in $\mathcal{C}^{\mathbb{A}}(\ell, m; r)^\perp$ does not depend on r as long as $r \geq 2$. The fact that $r \geq 2$ was used in the proofs several times. Therefore we have in fact shown that the set of minimum weight codewords in $\mathcal{C}^{\mathbb{A}}(\ell, m; r)^\perp$ equals the corresponding set in $\mathcal{C}^{\mathbb{A}}(\ell, m)^\perp$. Since the dimension of $\mathcal{C}^{\mathbb{A}}(\ell, m; r)^\perp$ does depend on r (see equation 1), this implies that $\mathcal{C}^{\mathbb{A}}(\ell, m; r)^\perp$ cannot possibly be generated by its minimum weight codewords if $r < \ell$. That they do if $r = \ell$ was established in [2] and with the above results, all such minimum weight codewords can be given explicitly. In the coming sections we will generalize these results to the Grassmann codes $\mathcal{C}(\ell, m)^\perp$.

3 Classification of minimum weight codewords of $\mathcal{C}(\ell, m)^{\perp}$.

The affine Grassmann codes investigated above were inspired by Grassmann codes, which are the topic of this section. We briefly introduce Grassmann codes from this point of view, linking them to affine Grassmann codes. The $\ell \times \ell'$ matrix $\mathbf{X}$ of δ indeterminates X_{ij} can be extended to an $\ell \times m$ matrix $\mathbf{X}' = (\mathbf{X}|\mathbf{I}_\ell)$. Recall here that $m = \ell + \ell'$. The reason for this is that then the set of all ℓ-minors of $\mathbf{X}'$ corresponds exactly to the set $\Delta_{\leq \ell}$ from Definition 2. A way to "homogenize" the matrix $\mathbf{X}'$ is to consider an $\ell \times m$ matrix $\mathbf{Y}$ of ℓm indeterminates whose first ℓ' columns form $\mathbf{X}$. A natural analogue of the set $\Delta_{\leq \ell}$ in this setting is the set of all $\ell \times \ell$ minors of $\mathbf{Y}$. We define this more formally in the following:

Definition 16 *Let $\ell \leq m$ and denote by $\boldsymbol{Y} = (Y_{ij})$ an $\ell \times m$ matrix whose entries are indeterminates Y_{ij}. Then for any $J \subset \{1, \ldots, m\}$ with $\#J = \ell$, we write $f_J := \det(\,(Y_{ij})_{i \in \{1,\ldots,\ell\},\, j \in J}\,)$ and denote by Λ_ℓ the set of all such minors of $\boldsymbol{Y}$. Further we denote by $\mathcal{F}_\ell$ the linear vector space generated by Λ_ℓ.*

As before we aim to define an evaluation code where the functions are taken from $\mathcal{F}_\ell$. We also need to establish the set of evaluation points, i.e. the set of matrices we wish to evaluate these functions in. A first idea could be to choose as set $\mathbb{M}_{\ell \times m}(\mathbb{F}_q)$, but this turns out to be a bad idea. Indeed, if $\mathbf{M} \in \mathbb{M}_{\ell \times m}(\mathbb{F}_q)$ and $\mathbf{A} \in \mathrm{GL}_\ell(\mathbb{F}_q)$, then $f(\mathbf{AM}) = \det \mathbf{A} f(\mathbf{M})$ for any $f \in \mathcal{F}_\ell$, and $f(\mathbf{M}) = 0$ whenever $\mathrm{rank}\mathbf{M} < \ell$. It is therefore better only to choose matrices $\mathbf{M}$ of full rank ℓ and to avoid matrices that have the same rowspace. It is now clear how the Grassmannian variety $\mathcal{G}_{\ell,m}$, which is defined as the set of all ℓ-dimensional subspaces of $\mathbb{F}_q^m$, comes in: For each element $V \in \mathcal{G}_{\ell,m}$ one chooses an $\ell \times m$ matrix $\mathbf{M}_V$ whose rowspace equals V. Once these matrices are fixed, we can define Grassmann codes from the evaluation code point of view:

Definition 17 *Let m be an integer and suppose $\ell \leq m$. Then we define*

$$\mathcal{C}(\ell, m) := \{\mathrm{ev}(f) \,|\, f \in \mathcal{F}_\ell\},$$

where $\mathrm{ev}(f) := (f(M_V))_{V \in \mathcal{G}_{\ell,m}}$.

The usual definition, which is equivalent to ours, uses the language of projective systems exploiting the Plücker embedding of $\mathcal{G}_{\ell,m}$ [8, 10, 11]. A different choice of the matrices $\mathbf{M}_V$ does not alter the code significantly, but produces an equivalent code with the same basic parameters (weight distribution, possible supports of codewords, etcetera). Therefore, we may choose the matrices $\mathbf{M}_V$ as we please. For general q, these parameters (length $n(\ell, m)$, dimension $k(\ell, m)$, and minimum distance $d(\ell, m)$) of $\mathcal{C}(\ell, m)$ were determined in [8]. These parameters are

$$n(\ell, m) = \begin{bmatrix} m \\ \ell \end{bmatrix}_q := \prod_{i=0}^{\ell-1} \frac{q^{m-i} - 1}{q^{\ell-i} - 1},$$

$$k(\ell, m) = \binom{m}{\ell}, \quad \text{and} \quad d(\ell, m) = q^{\ell(m-\ell)}.$$

Note that the length of the code is $\#\mathcal{G}_{\ell,m}$, which is well known to be equal to the Gaussian binomial coefficient given above. Note that the codes $\mathcal{C}(\ell, m)$ and $\mathcal{C}^{\mathbb{A}}(\ell, m)$ are closely related. To make this precise, let us assume that the matrices M_V are chosen of the form $(\mathbf{M}|\mathbf{I}_\ell)$ whenever this is possible (this is precisely if the projection $p_\ell(V)$ of V onto its last ℓ coordinates has dimension ℓ). Then the codeword obtained from $c \in \mathcal{C}(\ell, m)$ by deleting all coordinates indexed by $V \in \mathcal{G}_{\ell,m}$ such that $\dim p_\ell(V) < \ell$, is a codeword of $\mathcal{C}^{\mathbb{A}}(\ell, m)$. Therefore $\mathcal{C}^{\mathbb{A}}(\ell, m)$ can be

obtained from $\mathcal{C}(\ell, m)$ by puncturing in these coordinates. Just as we for the affine Grassmann codes assumed that $\ell \geq 2$ (since we assumed that $r \geq 2$), we will also in this section assume that $\ell \geq 2$. In the trivial case that $\ell = 1$, the code $\mathcal{C}(\ell, m)$ is a projective Reed–Muller code, whose parameters are well known. Since the dual of a projective Reed–Muller code again is a projective Reed–Muller code, also the dual code is well understood in this case. Another trivial case occurs when $\ell = m$. In this case the length of the Grassmann code is simply 1. Therefore we will always assume that $2 \leq \ell < m$ when considering Grassmann codes. Like in the previous section, we wish to study the dual code of the codes under consideration. Using Definition 17, we see that $c \in \mathbb{F}_q^{n(\ell,m)}$ is in $\mathcal{C}(\ell, m)^\perp$ if and only if

$$\sum_{V \in \mathcal{G}_{\ell,m}} c_V f_J(M_V) = 0, \tag{6}$$

for all $f_J \in \Lambda_\ell$. It is not hard to determine the minimum distance of $\mathcal{C}(\ell, m)^\perp$. We do so in the following lemma:

Lemma 18 *Let $2 \leq \ell < m$ be integers. The minimum distance $d_\perp(\ell, m)$ of $\mathcal{C}(\ell, m)^\perp$ satisfies*

$$d_\perp(\ell, m) = 3.$$

Proof. It is well known that the map from the Grassmannian $\mathcal{G}_{\ell,m}$ to $\mathbb{P}^{\binom{m}{\ell}-1}$ associating to a subspace V the Plücker coordinates of V, gives rise to a well-defined embedding. Therefore, $d_\perp(\ell, m) \neq 1$ (since then a subspace V would exist all of whose Plücker coordinates would be zero) and $d_\perp(\ell, m) \neq 2$ (since then two subspaces would exists with the same image under the above map). Therefore the lemma follows if we can produce a codeword in $\mathcal{C}(\ell, m)^\perp$ of weight three. For $a, b \in \mathbb{F}_q$, consider the $\ell \times m$ matrix

$$M_{a,b} := \begin{pmatrix} \mathbf{I}_{\ell-1} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & a & b & \mathbf{0} \end{pmatrix}.$$

For $(a, b) \neq (0, 0)$, we denote by $V_{a,b} \in \mathcal{G}_{\ell,m}$ the rowspace of $M_{a,b}$. For simplicity we assume that the matrix $M_{V_{a,b}}$ that was chosen when defining the Grassmann code equals $M_{a,b}$. Now we define $c \in \mathbb{F}_q^{n(\ell,m)}$ coordinate-wise as follows:

$$c_V := \begin{cases} 1 & \text{if } V = V_{1,0} \text{ or } V = V_{0,1}, \\ -1 & \text{if } V = V_{1,1}, \\ 0 & \text{otherwise.} \end{cases}$$

We will have finished the proof once we show that $c \in \mathcal{C}(\ell, m)^\perp$. However, for all except two $f \in \Lambda_\ell$ we have $f(M_{a,b}) = 0$. The only two exceptions are the ℓ-minors f_ℓ (resp. $f_{\ell+1}$) determined by the first ℓ (resp. the first $\ell - 1$ and the $(\ell + 1)$-st) columns. For these minors we have

$$f_\ell(M_{a,b}) = a \quad \text{and} \quad f_{\ell+1}(M_{a,b}) = b.$$

A direct verification now shows that for all $f \in \Lambda_\ell$ Equation (6) is satisfied, which implies that $c \in \mathcal{C}(\ell, m)^\perp$. ■

Note that there is no distinction between $q = 2$ and $q > 2$ in the statement of Lemma 18, making the Grassmann codes a slightly more regular class of codes than the affine Grassmann codes. In the proof of Lemma 18 three spaces of the form $V_{a,b}$ were chosen, but other choices would have been possible. To describe these possibilities (which are in fact all possibilities), we introduce the following:

Definition 19 *Assume that $\ell < m$ and let $Z \in \mathcal{G}_{\ell-1,m}$, $Z' \in \mathcal{G}_{\ell+1,m}$. Then the line of the Grassmannian $\pi_Z^{Z'}$ determined by Z and Z' is defined as follows:*

$$\pi_Z^{Z'} := \{W \in \mathcal{G}_{\ell,m} \mid Z \subseteq W \subseteq Z'\}.$$

We denote the set of all such lines of the Grassmannian by $\mathcal{L}(\mathcal{G}_{\ell,m})$.

Note that any such line contains $q+1$ elements. The terminology line is justified by the fact that under the Plücker embedding, the $q+1$ elements lie on a line inside the projective space. It is easy to count the number of possible lines in Definition 19, by first choosing Z', then $Z \subset Z'$. Reasoning like this one obtains:

$$\#\mathcal{L}(\mathcal{G}_{\ell,m}) = \begin{bmatrix} m \\ \ell+1 \end{bmatrix}_q \begin{bmatrix} \ell+1 \\ \ell-1 \end{bmatrix}_q = \begin{bmatrix} m \\ \ell \end{bmatrix}_q \frac{(q^{m-\ell}-1)(q^\ell-1)}{(q^2-1)(q-1)}. \tag{7}$$

The sets we have called lines of the Grassmannian, occur in the literature as well (see for example [4] and [9, Ch.2.2 Ex.2.5]).

Also note that the $q+1$ spaces $V_{a,b}$ (with $(a,b) \neq (0,0)$) form a line of the Grassmannian as in Definition 19 (one chooses $Z = V_{0,0}$ and $Z' = V_{1,0} + V_{0,1}$). It turns out that lines of a Grassmannian are the key to classify all minimum weight codewords in $\mathcal{C}(\ell,m)^\perp$. However, we first give a lemma.

Lemma 20 *Let $2 \leq \ell < m$ and let $\boldsymbol{G} \in \mathrm{GL}_m(\mathbb{F}_q)$. Then there exists $c \in \mathcal{C}(\ell,m)^\perp$ such that $\mathrm{supp}(c) = \{U,V,W\}$ if and only if there exist $c' \in \mathcal{C}(\ell,m)^\perp$ such that $\mathrm{supp}(c') = \{U \cdot \boldsymbol{G}, V \cdot \boldsymbol{G}, W \cdot \boldsymbol{G}\}$. Moreover, U,V and W lie on a line of the Grassmannian if and only if $U \cdot \boldsymbol{G}, V \cdot \boldsymbol{G}$ and $W \cdot \boldsymbol{G}$ lie on a line of the Grassmannian*

Proof. Note that right multiplication with $\mathbf{G}$ induces a permutation on $\mathcal{G}_{\ell,m}$. This permutation gives rise to an automorphism of $\mathcal{C}(\ell,m)$ (and hence of $\mathcal{C}(\ell,m)^\perp$). The proof of the last statement of the lemma is clear: U,V and W lie on $\pi_Z^{Z'}$ if and only if $U \cdot \mathbf{G}, V \cdot \mathbf{G}$ and $W \cdot \mathbf{G}$ lie on $\pi_{Z \cdot \mathbf{G}}^{Z' \cdot \mathbf{G}}$. ■ In the above proof some care needs to be taken in order to deal with the ambiguity when choosing the matrices $\mathbf{M}_V$ in Definition 17. This means that the automorphism induced by the permutation in the above proof will in general not be a permutation automorphism. See [5] for more details as well as a complete determination of the automorphism group. These details are not important when classifying minimum weight codewords, since these are (up to scaling) uniquely defined by their support sets. We are now ready to proceed with the main theorem of this section.

Theorem 21 *Let $2 \leq \ell < m$ and let $\{U,V,W\} \subset \mathcal{G}_{\ell,m}$. Then there exists a codeword $c \in \mathcal{C}(\ell,m)^\perp$ such that $\mathrm{supp}(c) = \{U,V,W\}$ if and only if U, V and W lie on a line of the Grassmannian.*

Proof. First assume that U,V and W lie on the same line $\pi_Z^{Z'}$. In this case it holds that $Z = U \cap V \cap W$ and $Z' = \mathrm{span}_{\mathbb{F}_q}(U,V,W)$. Therefore, there exist $\mathbf{x},\mathbf{y} \in \mathbb{F}_q^m$ such that $U = \mathrm{span}_{\mathbb{F}_q}(Z,\mathbf{x})$, $V = \mathrm{span}_{\mathbb{F}_q}(Z,\mathbf{y})$, $W = \mathrm{span}_{\mathbb{F}_q}(Z,\mathbf{x}+\mathbf{y})$, and $\mathrm{span}_{\mathbb{F}_q}(U,V,W) = \mathrm{span}_{\mathbb{F}_q}(Z,\mathbf{x},\mathbf{y})$. The choice of matrices $\mathbf{M}_U, \mathbf{M}_V$ and $\mathbf{M}_W$ in Definition 4 does not affect the supports of codewords, so when proving the theorem, we may choose these matrices as we wish. Using that U,V and W lie on the same line $\pi_Z^{Z'}$, we may choose $\mathbf{M}_U, \mathbf{M}_V$ and $\mathbf{M}_W$ such that they have the same $\ell-1$ rows (generating Z), but having $\mathbf{x}$, $\mathbf{y}$ and $\mathbf{x}+\mathbf{y}$ as final ℓ-th row. The multilinearity of the determinant then implies that $f(\mathbf{M}_U) + f(\mathbf{M}_V) - f(\mathbf{M}_W) = 0$ for any ℓ-minor $f \in \Lambda_\ell$. This implies that there exists a codeword in $c \in \mathcal{C}(\ell,m)^\perp$ such that $\mathrm{supp}(c) = \{U,V,W\}$.

Conversely, let U, V and W be three linear spaces in $\mathcal{G}_{\ell,m}$ such that U, V and W represent the nonzero positions of a minimum weight codeword $c \in \mathcal{C}(\ell,m)^\perp$. Given any choice for $\mathbf{M}_U$, there exists $\mathbf{G} \in \mathrm{GL}_m(\mathbb{F}_q)$ such that $\mathbf{M}_U\mathbf{G} = (\mathbf{I}_\ell|\mathbf{0})$. Using Lemma 20, we may assume without loss of generality that $\mathbf{M}_U = (\mathbf{I}_\ell|\mathbf{0})$. Now let $J := \{1, 2, \ldots, \ell\}$ and consider the ℓ-minor $f := f_J \in \Lambda_\ell$. Since $f(\mathbf{M}_U) = 1$ and c_U, c_V, c_W are nonzero, we may (possibly after interchanging V and W) assume that $f(\mathbf{M}_V) \neq 0$. Possibly after choosing a different matrix $\mathbf{M}_V$ with the same row space V, we may assume that $\mathbf{M}_V = (\mathbf{I}_\ell|\mathbf{N})$ for a suitable matrix $\mathbf{N}$. Note that $\mathbf{N} \neq \mathbf{0}$, since $U \neq V$. Applying Lemma 20 with $\mathbf{G}$ suitably chosen of the form $\mathbf{G} = \left(\begin{smallmatrix} \mathbf{I}_\ell & \mathbf{0} \\ \mathbf{C} & \mathbf{B} \end{smallmatrix}\right) \in \mathrm{GL}_m(\mathbb{F}_q)$, we may assume that $\mathbf{M}_U = (\mathbf{I}_\ell|\mathbf{0})$ and

$$\mathbf{M}_V = \left(\begin{array}{c|cccc} & n_{1,\ell+1} & n_{1,\ell+2} & \cdots & n_{1,m} \\ & \vdots & \vdots & & \vdots \\ & n_{i-1,\ell+1} & n_{i-1,\ell+2} & \cdots & n_{i-1,m} \\ \mathbf{I}_\ell & 1 & 0 & \cdots & 0 \\ & n_{i+1,\ell+1} & n_{i+1,\ell+2} & \cdots & n_{i+1,m} \\ & \vdots & \vdots & & \vdots \\ & n_{\ell,\ell+1} & n_{\ell,\ell+2} & \cdots & n_{\ell,m} \end{array}\right).$$

Now let $J' = (J \cup \{\ell+1\}) \setminus \{i\}$ and let $f' := f_{J'}$ be the ℓ-minor determined by the columns indexed by elements from J'. Then Equation (6) implies that $f'(\mathbf{M}_W) = -c_V f'(\mathbf{M}_V)/c_W \neq 0$. Therefore, possibly after choosing the matrix $\mathbf{M}_W$ differently (but keeping its rowspace fixed) we may assume that

$$\mathbf{M}_W = \left(\begin{array}{ccc|cccc} & o_{1,i} & & 0 & o_{1,\ell+2} & \cdots & o_{1,m} \\ \mathbf{I}_{i-1} & \vdots & \mathbf{0} & \vdots & \vdots & & \vdots \\ & o_{i-1,i} & & 0 & o_{i-1,\ell+2} & \cdots & o_{i-1,m} \\ 0\cdots0 & o_{i,i} & 0\cdots0 & 1 & o_{i,\ell+2} & \cdots & o_{i,m} \\ & o_{i+1,i} & & 0 & o_{i+1,\ell+2} & \cdots & o_{i+1,m} \\ \mathbf{0} & \vdots & \mathbf{I}_{\ell-i} & \vdots & \vdots & & \vdots \\ & o_{\ell,i} & & 0 & o_{\ell,\ell+2} & \cdots & o_{\ell,m} \end{array}\right).$$

With these choices of $\mathbf{M}_U$, $\mathbf{M}_V$ and $\mathbf{M}_W$ in place, Equation (6) applied to the minors f and f' as above, implies that $c_W = -c_V$ and $c_U + c_V + o_{i,i}c_W = 0$. Therefore, we may assume without loss of generality that $c_V = 1$, $c_W = -1$ and $c_U = o_{i,i} - 1$ (which in particular implies that $o_{i,i} \neq 1$).

Now we will use Equation (6) for other ℓ-minors to further determine the entries of $\mathbf{M}_V$ and $\mathbf{M}_W$. From now on in the proof we let $1 \leq j \leq \ell$, and $j \neq i$ and $\ell + 1 < j' \leq m$.

For $J^* = (J \cup \{j'\}) \setminus \{i\}$, Equation (6) implies that

$$0 = f_{J^*}(\mathbf{M}_V) - f_{J^*}(\mathbf{M}_W) = \pm(0 - o_{i,j'}) = \mp o_{i,j'}.$$

Therefore

$$o_{i,j'} = 0 \text{ for } j' > \ell + 1. \tag{8}$$

For $J^* = (J \cup \{\ell+1\}) \setminus \{j\}$, Equation (6) implies that

$$0 = f_{J^*}(\mathbf{M}_V) - f_{J^*}(\mathbf{M}_W) = \pm\left(\begin{vmatrix} 0 & n_{j,\ell+1} \\ 1 & n_{i,\ell+1} \end{vmatrix} - \begin{vmatrix} o_{j,i} & 0 \\ o_{i,i} & 1 \end{vmatrix}\right) = \mp(n_{j,\ell+1} + o_{j,i}).$$

Therefore

$$o_{j,i} = -n_{j,\ell+1} \text{ for } j \neq i. \tag{9}$$

For $J^* = (J \cup \{\ell+1, j'\}) \setminus \{i, j\}$, Equation (6) implies that

$$0 = f_{J^*}(\mathbf{M}_V) - f_{J^*}(\mathbf{M}_W) = \pm(n_{j,j'} - o_{j,j'}).$$

$$o_{j,j'} = n_{j,j'} \text{ for } j \neq i \text{ and } j' > \ell + 1. \tag{10}$$

Finally, for $J^* = (J \cup \{j'\}) \setminus \{j\}$, Equation (6) implies that

$$0 = f_{J^*}(\mathbf{M}_V) - f_{J^*}(\mathbf{M}_W) = \pm(n_{j,j'} - o_{i,i}o_{j,j'}) = \pm n_{j,j'}(1 - o_{i,i}),$$

where in the last equality we used Equation (10). We see that

$$n_{j,j'} = 0 \text{ for all } j \neq i \text{ and } j' > \ell + 1, \tag{11}$$

since we already have established that $o_{i,i} \neq 1$. Combining Equations (8),(9), (10) and (11) we see that

$$\mathbf{M}_V = \left(\begin{array}{c|ccc} & n_{1,\ell+1} & & \\ & \vdots & & \mathbf{0} \\ & n_{i-1,\ell+1} & & \\ \mathbf{I}_\ell & 1 & 0\cdots 0 & \\ & n_{i+1,\ell+1} & & \\ & \vdots & & \mathbf{0} \\ & n_{\ell,\ell+1} & & \end{array}\right).$$

and

$$\mathbf{M}_W = \left(\begin{array}{ccc|cccc} & -n_{1,\ell+1} & & 0 & & & \\ \mathbf{I}_{i-1} & \vdots & \mathbf{0} & \vdots & & \mathbf{0} & \\ & -n_{i-1,\ell+1} & & 0 & & & \\ 0\cdots 0 & o_{i,i} & 0\cdots 0 & 1 & 0 & \cdots & 0 \\ & -n_{i+1,\ell+1} & & 0 & & & \\ \mathbf{0} & \vdots & \mathbf{I}_{\ell-i} & \vdots & & \mathbf{0} & \\ & -n_{\ell,\ell+1} & & 0 & & & \end{array}\right).$$

In order to see ever more clearly how the rowspaces of $\mathbf{M}_U$, $\mathbf{M}_V$ and $\mathbf{M}_W$ are related, we redefine $\mathbf{M}_U$ (resp. $\mathbf{M}_V$) as the following matrix, which has the same rowspace as the original $\mathbf{M}_U$ (resp. $\mathbf{M}_V$):

$$\mathbf{M}_U = \left(\begin{array}{ccc|cccc} & -n_{1,\ell+1} & & 0 & & & \\ \mathbf{I}_{i-1} & \vdots & \mathbf{0} & \vdots & & \mathbf{0} & \\ & -n_{i-1,\ell+1} & & 0 & & & \\ 0\cdots 0 & 1 & 0\cdots 0 & 0 & 0 & \cdots & 0 \\ & -n_{i+1,\ell+1} & & 0 & & & \\ \mathbf{0} & \vdots & \mathbf{I}_{\ell-i} & \vdots & & \mathbf{0} & \\ & -n_{\ell,\ell+1} & & 0 & & & \end{array}\right),$$

$$\mathbf{M}_V = \left(\begin{array}{ccc|cccc} & -n_{1,\ell+1} & & 0 & & & \\ \mathbf{I}_{i-1} & \vdots & \mathbf{0} & \vdots & & \mathbf{0} & \\ & -n_{i-1,\ell+1} & & 0 & & & \\ 0\cdots 0 & 1 & 0\cdots 0 & 1 & 0 & \cdots & 0 \\ & -n_{i+1,\ell+1} & & 0 & & & \\ \mathbf{0} & \vdots & \mathbf{I}_{\ell-i} & \vdots & & \mathbf{0} & \\ & -n_{\ell,\ell+1} & & 0 & & & \end{array}\right).$$

With these choices for $\mathbf{M}_U$, $\mathbf{M}_V$ and $\mathbf{M}_W$ we can clearly identify and compare their rowspaces U, V and W. Note that all rows except the i-th row are the same for the three matrices. Therefore $\dim(U \cap V \cap W) = \ell - 1$. However, since the i-th row of $\mathbf{M}_U$ is a linear combination of the i-th rows of $\mathbf{M}_V$ and $\mathbf{M}_W$ the fact that $\dim \operatorname{span}_{\mathbb{F}_q}(U, V, W) = \ell + 1$ follows. Choosing $Z = U \cap V \cap W$ and $Z' = \operatorname{span}_{\mathbb{F}_q}(U, V, W)$, we see by Definition 19 that U, V and W lie on the line $\pi_Z^{Z'}$. The original U, V and W then also lie on a line of the Grassmannian by the second part of Lemma 20. ■ As a corollary we count the number of codewords of $\mathcal{C}(\ell, m)^\perp$ of weight 3.

Corollary 22 *Let $2 \leq \ell < m$. Then the code $\mathcal{C}(\ell, m)^\perp$ contains*

$$\frac{q(q^{m-\ell} - 1)(q^\ell - 1)}{6} \begin{bmatrix} m \\ \ell \end{bmatrix}_q$$

distinct codewords of weight 3.

Proof. Let $W \in \mathcal{G}_{\ell,m}$. By Equation (7), there are $\begin{bmatrix} m \\ \ell \end{bmatrix}_q \frac{(q^{m-\ell}-1)(q^\ell-1)}{(q^2-)(q-1)}$ distinct lines of the Grassmannian $\mathcal{G}_{\ell,m}$. Since a line contains $q+1$ elements of $\mathcal{G}_{\ell,m}$, there are $\binom{q+1}{3}$ subsets of the lines occurring as the support of a weight 3 codeword. For each such set there are $q-1$ codewords of weight 3 having this set as support set (no linearly independent minimum weight codewords with the same support set exist). Therefore, there are a total of

$$(q-1)\binom{q+1}{3} \begin{bmatrix} m \\ \ell \end{bmatrix}_q \frac{(q^{m-\ell} - 1)(q^\ell - 1)}{(q^2 - 1)(q - 1)}$$

of minimum weight codewords. ■

4 Generation by minimum weight codewords.

The investigation of the structure of the minimum weight codewords in $\mathcal{C}^{\mathbb{A}}(\ell, m)^\perp$ was motivated in [2] by a wish to decode $\mathcal{C}^{\mathbb{A}}(\ell, m)$, even though the ideal decoding algorithm is yet to be found. Especially the fact that $\mathcal{C}^{\mathbb{A}}(\ell, m)^\perp$ is generated by its minimum weight codewords, means that all information useful for decoding (syndromes, coset leaders, etcetera) is already obtained when considering the parity checks coming from such syndromes. This motivation also is one of the reasons to consider the similar question whether or not $\mathcal{C}(\ell, m)^\perp$ is generated by its weight 3 codewords. As we will show in this section, the answer is affirmative. The proof, like the ones in the previous section, exploits geometric properties of $\mathcal{G}_{\ell,m}$. We start with the following geometric concept:

Definition 23 *Let $0 \leq h \leq \ell \leq m$ be integers and let M be an $(m - \ell)$-dimensional linear subspace of $\mathbb{F}_q^m$. Then we define*

$$\mathcal{G}_{\ell,m}^h(M) := \{W \in \mathcal{G}_{\ell,m} \mid \dim(W \cap M) = h\}.$$

If $h > \min\{m - \ell, \ell\}$, then $\mathcal{G}_{\ell,m}^h(M) = \emptyset$. Note that given M, we may partition $\mathcal{G}_{\ell,m}$ with the sets $\mathcal{G}_{\ell,m}^h(M)$ for $h = 0, 1, \ldots, \ell$. Let us denote by $e_1, \ldots, e_m$ the standard basis vectors of $\mathbb{F}_q^m$. In the discussion after Definition 17, it was mentioned that $\mathcal{C}^{\mathbb{A}}(\ell, m)$ can be obtained from $\mathcal{C}(\ell, m)$ by puncturing in all coordinates indexed by spaces V whose projection $p_\ell(V)$ onto its last ℓ coordinates satisfies $\dim p_\ell(V) < \ell$. The remaining coordinates are indexed exactly by the

elements of $\mathcal{G}^0_{\ell,m}(\langle e_1,\ldots,e_{m-\ell}\rangle)$. In general $\mathcal{G}^0_{\ell,m}(M)$ is an affine part of the projective variety $\mathcal{G}_{\ell,m}$.

By adding zeros at the positions not in $\mathcal{G}^0_{\ell,m}(\langle e_1,\ldots,e_{m-\ell}\rangle)$, a codeword of $\mathcal{C}^{\mathbb{A}}(\ell,m)^\perp$ can be interpreted as a codeword of $\mathcal{C}(\ell,m)^\perp$. This identification will implicitly be made in the remainder of this section, whenever the codes $\mathcal{C}^{\mathbb{A}}(\ell,m)^\perp$ and $\mathcal{C}(\ell,m)^\perp$ are compared to each other. To show that $\mathcal{C}(\ell,m)^\perp$ is generated by its minimum weight codewords, we rely on Theorem 21. In order to exploit it fully, we first continue our study of triples lying on a line of the Grassmannian.

Lemma 24 *Let $W \in \mathcal{G}^h_{\ell,m}(M)$ where $0 < h \leq \min\{\ell, m-\ell\}$. Then there exist distinct $U, V \in \mathcal{G}^{h-1}_{\ell,m}(M)$ such that U, V and W lie on a line of the Grassmannian.*

Proof. Let $W \in \mathcal{G}^h_{\ell,m}(M)$. We may assume that W is of the form $\mathrm{span}_{\mathbb{F}_q}(T \cup \{y\})$ where $y \in M$ and $\dim T = \ell - 1$. Since $\dim T < \ell$ there exists x such that $x \notin \mathrm{span}_{\mathbb{F}_q}(M, T)$. This implies that the linear spaces $U = \mathrm{span}_{\mathbb{F}_q}(T \cup \{x+y\})$ and $V = \mathrm{span}_{\mathbb{F}_q}(T \cup \{x\})$ belong to $\mathcal{G}^{h-1}_{\ell,m}(M)$. ■

The last sentence of the proof could be replaced by: This implies that for any $\alpha \in \mathbb{F}_q \backslash \{0\}$, the linear spaces $U = \mathrm{span}_{\mathbb{F}_q}(T \cup \{\alpha x + y\})$ and $V = \mathrm{span}_{\mathbb{F}_q}(T \cup \{x\})$ belong to $\mathcal{G}^{h-1}_{\ell,m}(M)$. This shows that if $q > 2$ there is a considerable amount of choice for the linear spaces U and V. This will be used implicitly later on to avoid choosing U and V lying at infinity under the Plücker embedding. Now we consider the weight 4 codewords of $\mathcal{C}^{\mathbb{A}}(\ell,m)^\perp$ over $\mathbb{F}_2$ as codewords of $\mathcal{G}^\perp_{\ell,m}$ and give a description of them as the sum of two weight three codewords.

Lemma 25 *Let c be a weight 4 codeword in $\mathcal{C}^{\mathbb{A}}(\ell,m)^\perp$ over the binary field. Then the support of c is equal to the symmetric difference of two lines of the Grassmannian which have a common point.*

Proof.

From theorem 15 we know that the support of the weight 4 codewords of $\mathcal{C}^{\mathbb{A}}(\ell,m)^\perp$ over $\mathbb{F}_2$ follow in one of these cases.

- $\{\mathbf{0}, \mathbf{D}_1, \mathbf{E}_{1,2}, \mathbf{D}_1 + \mathbf{E}_{1,2}\}$
- $\{\mathbf{0}, \mathbf{D}_1, \mathbf{E}_{2,1}, \mathbf{D}_1 + \mathbf{E}_{2,1}\}$
- $\{\mathbf{0}, \mathbf{D}_1, \mathbf{E}_{1,2} + \mathbf{E}_{2,1}, \mathbf{D}_1 + \mathbf{E}_{1,2} + \mathbf{E}_{2,1}\}$

Note that the automorphism $\sigma_{\mathbf{U},\mathbf{I}_{m-\ell},\mathbf{I}_\ell}$ of $\mathcal{C}^{\mathbb{A}}(\ell,m)^\perp$ is induced by the induced automorphism $(\mathbf{X}|\mathbf{I}_\ell) \mapsto (\mathbf{X}|\mathbf{I}_\ell)\begin{pmatrix} \mathbf{I}_{m-\ell} & \mathbf{0} \\ \mathbf{U} & \mathbf{I}_\ell \end{pmatrix}$ of $\mathcal{C}(\ell,m)$. Additionally note that the automorphism $\sigma_{\mathbf{0},\mathbf{A},\mathbf{I}_\ell}$ of $\mathcal{C}^{\mathbb{A}}(\ell,m)^\perp$ is induced by $(\mathbf{X}|\mathbf{I}_\ell) \mapsto (\mathbf{X}|\mathbf{I}_\ell)\begin{pmatrix} \mathbf{A} & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_\ell \end{pmatrix}$ and the automorphism $\sigma_{\mathbf{0},\mathbf{I}_{m-\ell},\mathbf{B}}$ of $\mathcal{C}^{\mathbb{A}}(\ell,m)^\perp$ is induced by $(\mathbf{X}|\mathbf{I}_\ell) \mapsto (\mathbf{X}|\mathbf{I}_\ell)\begin{pmatrix} \mathbf{I}_\ell & \mathbf{0} \\ \mathbf{0} & \mathbf{B}^{-1} \end{pmatrix}$. Therefore the supports of the weight 4 codewords lie in the orbit under the automorphism group of $\mathcal{C}(\ell,m)^\perp$ of one of the following.

- $\{(\mathbf{0}|\mathbf{I}_\ell), (\mathbf{D}_1|\mathbf{I}_\ell), (\mathbf{E}_{1,2}|\mathbf{I}_\ell), (\mathbf{D}_1 + \mathbf{E}_{1,2}|\mathbf{I}_\ell)\}$
- $\{(\mathbf{0}|\mathbf{I}_\ell), (\mathbf{D}_1|\mathbf{I}_\ell), (\mathbf{E}_{2,1}|\mathbf{I}_\ell), (\mathbf{D}_1 + \mathbf{E}_{2,1}|\mathbf{I}_\ell)\}$
- $\{(\mathbf{0}|\mathbf{I}_\ell), (\mathbf{D}_1|\mathbf{I}_\ell), (\mathbf{E}_{1,2} + \mathbf{E}_{2,1}|\mathbf{I}_\ell), (\mathbf{D}_1 + \mathbf{E}_{1,2} + \mathbf{E}_{2,1}|\mathbf{I}_\ell)\}$

Note that the support sets are subsets of $\mathcal{G}^0_{\ell,m}(\langle e_1,\ldots,e_{m-\ell}\rangle)$. Each pair of spaces $\{(\mathbf{0}|\mathbf{I}_\ell), (\mathbf{D}_1|\mathbf{I}_\ell)\}$, $\{(\mathbf{E}_{1,2}|\mathbf{I}_\ell), (\mathbf{D}_1+\mathbf{E}_{1,2}|\mathbf{I}_\ell)\}$, $\{(\mathbf{E}_{2,1}|\mathbf{I}_\ell), (\mathbf{D}_1+\mathbf{E}_{2,1}|\mathbf{I}_\ell)\}$ and $\{(\mathbf{E}_{1,2}+\mathbf{E}_{2,1}|\mathbf{I}_\ell), (\mathbf{D}_1+\mathbf{E}_{1,2}+\mathbf{E}_{2,1}|\mathbf{I}_\ell)\}$ is contained in a line of $\mathcal{L}(\mathcal{G}_{\ell,m})$ and the third point of each line is $(\mathbf{D}_1|\mathbf{I}_\ell - \mathbf{D}_1)$. ■

Lemma 26 *Let c be a weight 3 codeword in $\mathcal{C}^{\mathbb{A}}(\ell,m)^{\perp}$ over a nonbinary field. Then the support of c is a set of 3 points on a line of $\mathcal{G}_{\ell,m}$.*

Proof.

From Theorem 8 we know that the support of the weight 3 codewords of $\mathcal{C}^{\mathbb{A}}(\ell,m)^{\perp}$ over $\mathbb{F}_q$ is equal to $\{\mathbf{0},\mathbf{M},\alpha\mathbf{M}\}$, where $\mathbf{M}$ has rank 1. As we saw in the proof of Lemma 25 we may consider the group of induced automorphisms $\mathfrak{H}(\ell,m)$ as the group of automorphisms of $\mathcal{G}_{\ell,m}$ generated by $\left(\begin{smallmatrix}\mathbf{I}_{m-\ell} & \mathbf{0}\\ \mathbf{U} & \mathbf{I}_\ell\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}\mathbf{A} & \mathbf{0}\\ \mathbf{0} & \mathbf{I}_\ell\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}\mathbf{I}_\ell & \mathbf{0}\\ \mathbf{0} & \mathbf{B}^{-1}\end{smallmatrix}\right)$. We may then apply an automorphism from $\mathfrak{H}(\ell,m)$ to obtain the set $\{\mathbf{0},\mathbf{E}_{1,1},\alpha\mathbf{E}_{1,1}\}$. Considering the corresponding positions in $\mathcal{G}_{\ell,m}$ given by the matrices $\{(\mathbf{0}|\mathbf{I}_\ell),(\mathbf{E}_{1,1}|\mathbf{I}_\ell),(\alpha\mathbf{E}_{1,1}|\mathbf{I}_\ell)\}$, we conclude that these three points lie on the same line. ■

From the previous results, we deduce the main theorem of this section:

Theorem 27 *The code $\mathcal{C}(\ell,m)^{\perp}$ is generated by its minimum weight codewords.*

Proof. Let $W\in\mathcal{G}_{\ell,m}$. We know from Theorem 6 and Lemma 26 (for $q=2$ Lemma 25) that the code $\mathcal{C}^{\mathbb{A}}(\ell,m)^{\perp}$ is generated by weight 3 codewords of $\mathcal{C}(\ell,m)^{\perp}$. Let $h>0$. Then for each $W\in\mathcal{G}^h_{\ell,m}$ we can find a codeword of weight 3 of $\mathcal{C}(\ell,m)^{\perp}$ whose other two positions in its support lie in $\mathcal{G}^{h-1}_{\ell,m}$. This implies that we have $\#\mathcal{G}_{\ell,m}-\#\mathcal{G}^0_{\ell,m}(M)$ independent codewords of weight 3, in addition to those from $\mathcal{C}^{\mathbb{A}}(\ell,m)^{\perp}$. Therefore $\mathcal{C}(\ell,m)^{\perp}$ is generated by its weight 3 codewords. ■

We finish the article by harvesting a consequence of the above explicit results on the weight three codewords for the generalized Hamming weights of $\mathcal{C}(\ell,m)^{\perp}$ and $\mathcal{C}^{\mathbb{A}}(\ell,m)^{\perp}$. The tool to achieve these results is stated in the following:

Theorem 28 *Let D be a subcode of $\mathcal{C}(\ell,m)^{\perp}$ where D does not have dimension 0, nor is it the full code. Then there exists $x\in\mathcal{C}(\ell,m)^{\perp}$ such that $\operatorname{span}_{\mathbb{F}_q}(D\cup x)$ has support either $\#supp(D)+1$ or $\#supp(D)+2$.*

Proof. The conditions on D imply $\{\}\neq supp(D)\neq\mathcal{G}_{m,\ell}$. Therefore there exist $U\in\operatorname{supp}(D)$ and $W\notin\operatorname{supp}(D)$. Since we can find a sequence of $V_1,V_2,\dots V_n$ such that $V_i\in\mathcal{G}_{\ell,m}$, $V_1=U$, $V_n=W$ and $\dim V_i\cap V_{i-1}=\ell-1$ we may assume $\dim U\cap W=\ell-1$. (In the sequence $V_1,V_2,\dots V_n$ there must be two consecutive elements such that one is in $\operatorname{supp}(D)$ and the other one is not.) If x is a codeword of weight 3 of $\mathcal{C}(\ell,m)^{\perp}$ which has support in U and W then $\operatorname{supp}(x)=\{U,V,W\}$, and $\operatorname{supp}(\operatorname{span}_{\mathbb{F}_q}(D\cup x))=\operatorname{supp}(D)\cup\operatorname{supp}(x)$ which finishes the proof. ■

Corollary 29 *The generalized Hamming weights of $\mathcal{C}(\ell,m)^{\perp}$ satisfy:*

$$d_{i+1}-d_i\in\{1,2\}$$

as long as $d_{i+1}\neq\begin{bmatrix}m\\ \ell\end{bmatrix}_q$.

Proof. This follows directly from Theorem 28: given a subspace of dimension i of weight d_i, we may construct a subspace of dimension $i+1$ whose support increases by at most 2. ■

Corollary 30 *For $q>2$, the generalized Hamming weights of $\mathcal{C}^{\mathbb{A}}(\ell,m;r)^{\perp}$ satisfy:*

$$d_{i+1}-d_i\in\{1,2\}$$

as long as $d_{i+1}\neq\begin{bmatrix}m\\ \ell\end{bmatrix}_q$.

Proof. The proof is very similar to that of the previous corollary. The only additional ingredient is that since $q>2$, the linear spaces V and W in the proof of Theorem 28 can be chosen from $\mathcal{G}^0_{\ell,m}(\langle e_1,\dots,e_{m-\ell}\rangle)$. ■

Acknowledgements

We would like to thank professor Sudhir R. Ghorpade for pleasant discussions on several topics related to Grassmann codes.

References

[1] P. Beelen, S. R. Ghorpade, and T. Høholdt, Affine Grassmann codes, IEEE Transactions on Information theory, vol. 56 (7), pp. 3166–3176 (2010).

[2] P. Beelen, S. R. Ghorpade, and T. Høholdt, Duals of affine Grassmann codes and their relatives, IEEE Transactions on Information theory, vol. 58 (6), pp. 3843–3855 (2012).

[3] S. R. Ghorpade and G. Lachaud, Higher weights of Grassmann codes, in Coding Theory, Cryptography and Related Areas (Guanajuato, 1998), pp. 122–131, Springer Verlag, Berlin/Heidelberg (2000).

[4] S. R. Ghorpade, A. R. Patil, and H. K. Pillai, Decomposable subspaces, linear sections of Grassmann varieties, and higher weights of Grassmann codes, Finite Fields and Applications, vol. 15, pp. 54–68 (2009).

[5] S. R. Ghorpade and K. V. Kaipa, Automorphism groups of Grassmann codes, Finite Fields and Applications, vol. 23, pp. 80–102, 2013.

[6] J. P. Hansen, T. Johnsen, and K. Ranestad, Grassmann codes and Schubert unions, in Arithmetic, Geometry and Coding Theory (Luminy, 2005), Séminaires et Congrès, vol. 21, pp. 103–121, Soc. Math. France, Paris (2009).

[7] F. J. MacWilliams and N. J. A. Sloane, The theory of error-correcting codes, North-Holland Publishing Company, Amsterdam, 1977.

[8] D. Y. Nogin, Codes associated to Grassmannians, in Arithmetic, Geometry and Coding Theory (Luminy, 1993), pp. 145–154, Walter de Gruyter, Berlin (1996).

[9] M. Pankov, Grassmannians of classical buildings, World Scientific, 2010.

[10] C. T. Ryan, An application of Grassmannian varieties to coding theory, Congr. Numerantium, vol. 57, pp. 257–271 (1987).

[11] C. T. Ryan, Projective codes based on Grassmannian varieties, Congr. Numerantium, vol. 57, pp. 273–279 (1987).

[12] C. T. Ryan and K. M. Ryan, The minimum weight of the Grassmann codes $C(k, n)$, Discrete Applied Mathematics, vol. 28 (2), pp. 149–156 (1990).